Las Técnicas de la Ingeniería Social como Factor de Riesgo en la Seguridad Informática

Dora Araceli Cruz Huerta [1]

Introducción

El activo más valioso para toda organización, es la información; hoy día, al compartir información con otra entidad a través de las nuevas tecnologías, se corre el riesgo de ser víctima de una invasión a la privacidad.

Por tal motivo las instituciones gubernamentales, educativas y financieras, principalmente, implementan cada vez mayores controles de seguridad para proteger su información, como son circuitos de cámaras, cajas fuertes, firewalls, entre otros.

Acerca de la autora...

[1] Maestra en Ciencias, docente de la División de Informática del Tecnológico de Estudios Superiores de Ecatepec

Sin embargo, un aspecto importante a considerar es el ser humano, que almacena información muy sensible y que por olvido o reto, asegura la información dentro de su cerebro, no prestando mucha atención a este aspecto. Pero siempre existirá un riesgo humano presente y por lo tanto vulnerable a la ingeniería social.

Desde que surgieron las tecnologías de la información (TI), la seguridad informática ha sido necesaria, ya que busca satisfacer las necesidades de los usuarios y con ello los medios para cuidar y resguardar la información, tomando en cuenta que a partir de que surgen los virus y los ataques cibernéticos, la seguridad informática juega un papel importante en nuestras vidas.

Hay que considerar que las tecnologías de la información son herramientas y métodos que nos permiten manejar y distribuir datos de manera vertiginosa, y que actualmente se usan en cualquier campo a través de Internet, tarjetas de crédito, pagos electrónicos, entre otras funciones, que ofrecen ventajas competitivas, como el disponer de cursos y recursos alternativos de acción para adaptarlos a las necesidades del momento.

La importancia de la presente investigación es dar a conocer a los estudiantes, los problemas que crea de la ingeniería social, ya que tarde o temprano se enfrentarán al arte de manipular para eludir los sistemas de seguridad, por lo que es necesario enseñarles a agilizar su sentido común, para no poner en peligro la seguridad propia y su integridad.

Seguridad informática vs ingeniería social

En este trabajo se analizó lo que es la seguridad informática y la ingeniería social, así como también se proponen acciones para mitigarla en la medida de lo posible o por lo menos darla a conocer, ya que muchas personas desconocen su significado y comportamiento.

Cabe mencionar que la ingeniería social es la pericia de obtener información confidencial a través de la manipulación de usuarios legítimos. Esta estrategia la pueden usar para obtener información de manera positiva y en la mayoría de los casos de manera negativa; los investigadores privados, criminales o delincuentes informáticos, buscan tener acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgos o abusos, lo cual es considerado como un problema muy serio y preocupante.

La ingeniería social es el punto débil de los sistemas informáticos, ya que un ingeniero social usará comúnmente el teléfono o internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de alguna dependencia de salud o empresa, un compañero de trabajo, un técnico o un cliente, para solicitarle la renovación de permisos de accesos a páginas web o verificación de datos mediante preguntas engañosas e incluso las conocidas cadenas, a fin de que la víctima revele información sensible o viole las políticas de seguridad. Estos sujetos aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones cuando se le pide revelar detalles financieros aparentemente por parte de un ejecutivo de un banco o una institución.

A menudo se dice que la única computadora segura es aquella que nunca será encendida. El hecho que se pueda persuadir a alguien para que le suministre por ejemplo su número de tarjeta de crédito, puede sonar como algo poco factible, sin embargo, las personas suministran datos confidenciales diariamente por distintos medios, como el papel que arroja a la basura o el sticker adhesivo con su password (contraseña) debajo del teclado, por lo que el factor humano es una parte esencial del juego de seguridad.

No existe un sistema informático que no dependa de algún dato ingresado por el humano. Esto significa que esta debilidad en la seguridad es universal, independiente de la plataforma, el software, la red o edad del equipo en cuestión.

Otros de los posibles ataques puede ser simple, pero efectivo, al engañar a un usuario llevándolo a pensar que es un administrador del sistema quien le está solicitando una contraseña para varios propósitos legítimos; los usuarios de sistemas de internet reciben mensajes donde le solicitan contraseñas o información de su tarjeta de crédito, ya sea para crear una cuenta, reactivar una configuración u efectuar alguna operación. A este tipo de ataques se les llama phishing (se pronuncia igual que fishing, pesca), por tal motivo es necesario alertar a las personas para que no divulguen contraseñas u otra información sensible a personas que dicen ser administradores, ya que ellos no necesitan saber la contraseña de los usuarios para llevar a cabo sus tareas, y esta falta de conocimiento nos hace vulnerables ante el ataque.

Por ejemplo, encuesta realizada por la empresa Boixnet, reveló que 90% de los empleados de oficina de la estación Waterloo en Londres, revelaron sus contraseñas a cambio de un bolígrafo barato; parece increíble, pero es toda una realidad.

El pishing se puede aplicar por correo electrónico o hasta en redes sociales. Prácticamente todos en algún momento hemos recibido un email procedente de “nuestro banco” solicitando contraseñas, confirmación de nombres de usuarios, o números de cuenta y tarjetas de crédito. Los bancos nunca solicitan información por correo y jamás debemos enviarla por este medio, y mucho menos dar nuestra clave que aparece al reverso de la tarjeta. Muchos emails de este tipo, incluyen enlaces a sitios fraudulentos o que engañan al receptor bajo el pretexto de ser una empresa legítima que intenta verificar nuestros datos.

El éxito de estos ataques radica en que los humanos simplemente somos susceptibles a la manipulación y podemos ser persuadidos para hacer muchas cosas, si se presionan los botones correctos.

Defensa contra la Ingeniería Social

La principal defensa contra la Ingeniería Social es educar y entrenar a los alumnos y usuarios en la aplicación de políticas de seguridad y asegurarse de que éstas sean realmente seguras. Es necesario educar a todos, desde los trabajan transmitiendo datos, los operarios, hasta el personal de limpieza, que pudiera ser el más susceptible de proporcionar información, sin saber que pueden perjudicar a terceros.

Antes de abrir los correos, debemos analizarlos con un antivirus eficaz y debidamente actualizado, ya que cualquier mensaje de correo electrónico puede contener códigos maliciosos aunque no le acompañe el símbolo de datos adjuntos o de una posible amenaza de virus. Nunca se debe ejecutar un programa de procedencia desconocida, aun cuando previamente sea verificado que no contiene virus. Dicho programa puede contener un troyano o un sniffer que reenvíe nuestra clave de acceso.

No debemos informar telefónicamente sobre las características técnicas de la red, ni el nombre de personal a cargo. Lo adecuado es remitirlos directamente al responsable (administrador de la red); asimismo, crear un control de acceso físico al sitio donde se encuentren los equipos (rack), y establecer políticas de seguridad a nivel del sistema operativo, como lo muestra la Figura 1.

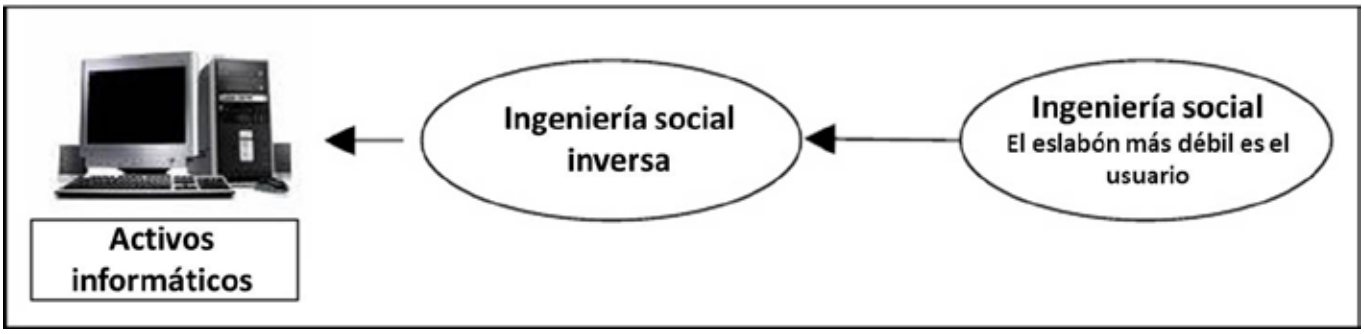

Figura 1

Control de acceso físico.

Técnicas de Ingeniería Social

Existen tres tipos de técnicas según el nivel de interacción del ingeniero social:

Técnicas pasivas

Observación

Técnicas no presenciales

Recuperar la contraseña

IRC u otros chats.

Teléfonos.

Cartas y fax.

Técnicas presenciales no agresivas

Buscar en la basura.

Seguimiento de personas y vehículos.

Vigilancia de edificios.

Inducción.

Entrada en hospitales.

Acreditaciones.

Agendas y teléfonos móviles.

Desinformación.

Métodos utilizados por los atacantes

Son varios los métodos que un atacante puede utilizar para conseguir que se le brinde información o se le facilite el acceso a un sistema restringido, aunque lo más común es que utilice una mezcla de todos los recursos existentes.

Métodos agresivos

Suplantación de personalidad.

Chantaje o extorsión.

Despersonalización.

Presión psicológica.

Relación de la ingeniería social con la seguridad informática

La seguridad informática tiene por objetivo asegurar que los datos almacenados en nuestros ordenadores se mantengan libres de cualquier problema, y que el servicio que brinden dichos sistemas se realice con la mayor efectividad. En este sentido, la seguridad informática abarca cosas tan dispares como:

Los aparatos de aire acondicionado que los mantienen a las temperaturas adecuadas para trabajar sin problemas.

La calificación del equipo de administradores, quienes deberán conocer lo suficiente como para mantenerlo funcionando correctamente.

La definición de entornos en donde las copias de seguridad han de guardarse para mantenerlas resguardadas y cómo hacer esas copias.

El control del acceso físico a los sistemas.

La elección de un hardware y de un software que no dé problemas.

La correcta formación de los usuarios del sistema.

El desarrollo de planes de contingencia.

Amenazas

Los sistemas informáticos suelen ser vulnerables a múltiples amenazas, que pueden ocasionar daños que representen pérdidas significativas. Los daños pueden variar desde simples errores en el uso de aplicaciones de gestión que comprometan la integridad de los datos, hasta catástrofes que inutilicen la totalidad de los sistemas.

Las pérdidas pueden aparecer por la actividad de intrusos externos a la organización o empresa, por accesos fraudulentos, por accesos no autorizados, por el uso erróneo de los sistemas por parte de empleados, o por la aparición de eventualidades destructivas.

Formas de ataque

Las formas de ataque son muy variadas y dependen de la imaginación del agresor y sus intereses. En general, los ataques de Ingeniería Social operan en dos niveles: el físico y el psicosocial. El primero describe los recursos y medios a través de los cuales se llevará a cabo el ataque, y el segundo es el método con el que se engañará a la víctima.

Las formas usadas a nivel físico son:

Ataque por teléfono. Es la forma más persistente de Ingeniería Social. En ella el perpetrador realiza una llamada telefónica a la víctima, haciéndose pasar por alguien conocido, como un técnico de soporte o un empleado de la misma organización. Es un modo muy efectivo, pues las expresiones del rostro no son reveladas y lo único que se requiere es un teléfono.

Ataque vía Internet. Desde que Internet se convirtió uno de los medios de comunicación más importantes, la variedad de ataques en red se incrementó en igual medida que los servicios existentes. Los ataques más comunes son vía correo electrónico o inclusive conversando con personas específicas en salas de chat y servicios de mensajería.

Dumpster Diving o Trashing (zambullida en la basura**).** Consiste en buscar información relevante en la basura, como agendas telefónicas, organigramas, agendas de trabajo, unidades de almacenamiento (CD, USB), entre otros.

Ataque vía SMS o WhatsApp. Aprovecha las aplicaciones de los celulares. El intruso envía un mensaje SMS o un WhatsApp a la víctima, haciéndola creer que el mensaje es parte de una promoción o un servicio; luego, si la persona lo responde, puede revelar información personal, y ser víctima de robo o dar pie a una estafa más elaborada.

Ataque vía correo postal. Es uno de los ataques donde la víctima se siente más segura, principalmente por la fiabilidad del correo postal. El perpetrador envía un correo falso a la víctima, tomando como patrón alguna suscripción de una revista, cupones de descuento, etcétera. La propuesta se diseña de manera atractiva, para que la víctima, si todo sale bien, responda al apartado postal del atacante enviándole todos sus datos.

Ataque cara a cara. Es el método más eficiente, pero a la vez el más difícil de realizar. El perpetrador requiere tener una gran habilidad social y extensos conocimientos para poder manejar adecuadamente cualquier situación que se le presente. Las personas más susceptibles suelen ser las más “inocentes”, por lo que no es un gran reto para el atacante cumplir su objetivo si elige bien a su víctima, a través de haberla estudiado sin que se dé cuenta.

Por otro lado, existen entornos psicológicos y sociales que pueden influir para que un ataque de ingeniería social sea exitoso. Algunos de ellos, son:

Exploit de familiaridad. Táctica en que el atacante aprovecha la confianza que la gente tiene en sus amigos y familiares, haciéndose pasar por cualquiera de ellos. Un ejemplo claro de esto ocurre cuando un conocido llega a una fiesta acompañado de un amigo. En una situación normal nadie dudaría de que ese individuo pudiera no ser de confianza. Pero ¿en verdad podemos confiar en alguien a quien jamás hemos tratado? Son preguntas que debemos plantearnos.

Crear una situación hostil. El ser humano siempre procura alejarse de aquellos que parecen estar locos o enojados, o en todo caso, salir de su camino lo antes posible. Crear una situación hostil justo antes de un punto de control en el que hay vigilantes, provoca el suficiente estrés para no revisar al intruso o responder sus preguntas y de esa manera pasar inadvertido.

Conseguir empleo en el mismo lugar. Cuando la recompensa lo amerita, estar cerca de la víctima puede ser una buena estrategia para obtener toda la información necesaria. Aunque hoy día se aplican varios filtros para ser contratados, todavía hay pequeñas y medianas empresas que no realizan una revisión meticulosa de los antecedentes de un nuevo solicitante, por lo que obtener un empleo donde la víctima labora puede resultar fácil.

A continuación se cita los casos de dos empresas en México sobre la seguridad y ataques de la Ingeniería Social

Caso 1

Empresa VEXILIO, ubicada en la colonia Barrio de San Lucas, Delegación Coyoacán. Es una empresa desarrolladora de software 100% Mexicana con la más alta tecnología, y su filosofía es que cada sistema que desarrolle, logre su objetivo permitiendo que sea robusto, seguro y que proporcione no solo los resultados esperados sino ir más allá.

Concerniente a la Ingeniería Social, comentan que hace tiempo fueron atacados a través de un Tailgaiting, un recurso que se aprovecha de la solidaridad y buena voluntad, generalmente suele ejecutarse cuando un empleado (la víctima) está ingresando a su empresa, la cual posee algún tipo de restricción en su acceso físico. Por ejemplo tarjetas RFID para torniquetes (barrera de acceso).

El atacante irá corriendo con una gran sonrisa detrás de la víctima justo antes de que éste termine de ingresar, haciendo un gesto de haber olvidado su tarjeta de acceso, en caso de existir un torniquete, ingresará junto a la víctima, disculpándose por su torpeza y de esa manera lograr introducirse.

Por eso es importante no confiar plenamente en las personas, ya que aunque haya contratos legales de por medio, aún así se llegan a presentar robos de información.

Para ello se aplican exámenes de confianza y capacitación del personal sobre la Ingeniería Social. Recomiendan no comentar o compartir datos sobre sus gustos y afinidades, para que no los usen en su contra.

Caso2

Royal Holiday Club (o **Royal Holiday**) es un operador de membrecías de club de vacaciones, y desarrollador de complejos turísticos con sede en México, que ofrece venta de vacaciones bajo un sistema de puntos, los cuales pueden ser cambiados por alojamiento, amenidades y entretenimiento en aproximadamente 180 puntos en América del Norte, América del Sur, África, Europa y Asia. La compañía implementa una política a través de la cual sus miembros pueden "prestarse" sus puntos entre ellos. Royal Holiday es propietario y opera diez de sus hoteles, ocho de ellos en México, uno en Puerto Rico y otro en Argentina. Fue fundada en México en 1983 como una compañía privada dedicada a la hospitalidad, Royal Holiday Club abrió sus oficinas de ventas inicialmente en Cancún y Cozumel, en 1985. En 2010, la compañía empleaba alrededor de 3,500 personas, y tenía cerca de 110,000 socios provenientes de 52 países. Su presidente es Pablo González Carbonnell, y Rosario Rodríguez Rojo es la Directora General.

Royal Holiday Club inicialmente perteneció a una compañía de hospitalidad y bienes raíces llamada en ese entonces Costamex Group. Al final de la década de 1980, Royal Holiday Club consolidó una tendencia a la expansión, en conjunto con complejos en Norte América, América del Sur, África, Europa y Asia. Royal Holiday Club en esa época comenzó a remodelar o construir varios de sus hoteles "Park Royal", incluyendo dos en Cancún. Bloomberg Businessweek describe a la compañía propietaria de Royal Holiday Club como la dueña y operadora de una cadena de hoteles que "ofrecen regímenes de pensiones, alojamiento, y servicios de entretenimiento y recreación".

En ese tiempo, la compañía no había "arribado todavía" a su estrategia expansiva, según testimonio de González Carbonnell, quien agregó que seguían buscando oportunidades fuera de México. En 1994, las ventas acumuladas de propiedades de vacaciones en los Estados Unidos, fue liderada por Marriott con $225 millones, seguida por Westgate Resorts ($120 millones), y Royal Holiday Club en tercer lugar, con ventas totales por $110 millones. Al cabo de 1994, Royal Holiday Club llevaba acumuladas ventas mundiales por $481 millones.

Enfocándose a la ingeniería social, Royal utiliza el software Travelio, que consta de un sistema desarrollado por la empresa, que facilita la gestión de todos los procesos y tareas inherentes, como facturación, gestión de reservas, contrataciones entre otros servicios.

Travelio utiliza tecnologías y estándares (Web Services) que le permiten ser implantado en cualquier servidor de aplicaciones J2EE y base de datos.

Concerniente a la Ingeniería Social, los empleados del hotel tienen una maestría en ella. Este arte puede ser utilizado para bien, proporcionando a los huéspedes un servicio excepcional, en relación con la conciencia de

seguridad; este conjunto de habilidades de los empleados se ve reforzado y les da una ventaja frente a los depredadores criminales.

Los hoteles ya tienen una gran trayectoria en la que pueden basarse, debido a la naturaleza del negocio. Con la capacitación y reforzamiento del personal en habilidades de servicio que ya poseen y la formación de éstos sobre educación de inseguridad, los hoteles tienen una potente solución para frustrar los ataques de phishing y las tácticas de ingeniería social de los delincuentes.

Por ejemplo, el botones que acompaña al huésped a la habitación, se da cuenta que el huésped tiene una pasión por los caballos. Al día siguiente, el huésped encuentra una revista acerca de la equitación en su habitación. O el camarero en la terraza de la piscina, que se da cuenta que la pequeña hija de un cliente ama las fresas, como un pequeño capricho el trae un tazoncito de fresas solo para ella. La madre está impresionada con él y la hospitalidad de primera clase. Este es un buen servicio, debido a que todo el personal está prestando atención a los detalles. Ese es el fundamento de la ingeniería social.

Por otro lado, los criminales de este tipo no usan pasamontañas, en cambio, tratan de mezclarse con los huéspedes y el personal del hotel. También usan diversas técnicas de ingeniería social para conectarse con sus víctimas y extraer la información confidencial que necesitan para cometer delitos.

Como otro ejemplo, tenemos a un hombre que está acechando a una de las clientas en un hotel. La joven de la habitación 305 no lo conoce, pero ella lo ha visto antes fuera de hotel. Él la sigue y trata de acecharla un par de veces desde el bar, pero no tiene éxito. Cuando ella desaparece al retirarse a su habitación, el acosador se acerca a la recepción. Él quiere información acerca de la chica, por lo que involucra al recepcionista en la conversación. Pero no comienza haciendo preguntas acerca de la dama, eso crearía sospechas. El primer intento se tratar de construir una relación empática con el recepcionista. Lo hace para que el empleado empiece a confiar en él. Hasta ahora se involucra en una pequeña charla. Luego investiga acerca de la mujer que le interesa. Él pregunta de dónde es y cuánto tiempo se hospeda en el hotel, lo cual le ayudará a recrear su perfil más tarde y hacer planes para su próximo movimiento. Posiblemente, él no tiene un plan todavía. Incluso puede pretender conocerla.

Sin embargo, el recepcionista hace lo correcto y lo identifica como persona sospechosa. El recepcionista se acuerda del curso de Conciencia de Seguridad que recientemente completó. Con el fin de crear una distracción y para ganar tiempo, el recepcionista da información falsa, diciendo al acosador que la dama se hospeda en el hotel con su marido. Ahora el recepcionista está utilizando la ingeniería social para enfriar a un atacante potencial. El recepcionista informa inmediatamente del incidente al gerente de turno, quien discretamente lo hará del conocimiento de la dama. Él le ofrece un cambio de habitación para su propia seguridad y también cambiar su nombre en el sistema, si así lo quiere. El gerente, a continuación, se presenta al acosador y le pregunta si está siendo atendido.

Esa es también una forma excepcional de servicio al cliente. El acosador se da cuenta que ha sido descubierto y es de esperar que ahora se dará por vencido en sus intenciones y se marche.

Habrá señales de debilidad en el acosador que lo delaten. Si fuese un depredador sexual, va a mostrar signos de nerviosismo. Posiblemente evitará el contacto visual, sobre todo si está haciendo esto por primera vez.

Caso 3

Kevin Mitnick, nacido en Los Ángeles (EE.UU.) en 1963, fue quien impulsó e hizo conocido el concepto de Ingeniería Social dentro del mundo IT. Ya a los 16 años de edad rompió la seguridad en el sistema administrativo de su colegio, sólo para curiosear y divertirse.

Su primera infracción a la Ley fue en 1981, al entrar físicamente en las oficinas de la empresa COSMOS (Computer System for Mainframe Operations), perteneciente a Pacific Bell. Allí, junto con dos amigos, robaron información muy valiosa de la empresa, valuada en 200,000 dólares. Inmediatamente fueron delatados por la novia de uno de los amigos y tiempo después capturados y sentenciados a tres meses de prisión, además de un año de libertad condicional. Al tener un espíritu "inquieto", Kevin siguió haciendo de las suyas: al oficial asignado para su custodia, alguien le dio de baja su línea telefónica y la compañía no tenía registro alguno de lo sucedido.

A medida que pasaba el tiempo, los objetivos de Mitnick iban creciendo. Una de las acciones que lo lanzó a la fama, fue el tener acceso secreto durante varios meses al correo electrónico de los miembros del Departamento de Seguridad de MCI Communications y Digital Equipment Corporation. Esto lo realizó para conocer cómo estaban protegidos sus equipos y sus sistemas telefónicos. Luego de una ardua recolección de información, Mitnick pudo hacerse de códigos para entrar junto con un amigo a la red del laboratorio de investigaciones de la Corporación. Su objetivo final era poder hacerse de un nuevo prototipo de un sistema operativo. Personal del laboratorio advirtió sobre el ataque al FBI e inmediatamente comenzó un rastreo.

Mitnick fue arrestado en 1988 por invadir y causar daños por 4 millones de dólares a la empresa, siendo culpable por los cargos de fraude y posesión ilegal de códigos de acceso de larga distancia. Fue tal la fama que ganó Mitnick, que adicionalmente a la sentencia el fiscal solicitó una orden a la corte para que le prohibiera acceder a cualquier teléfono.

De alguna manera, Mitnick consiguió que su abogado también usara Ingeniería Social. La táctica que presentó para reducir la condena fue alegar que su cliente sufría de adicción a las computadoras. Así, la condena se redujo notablemente a sólo un año de prisión y luego seis meses de tratamiento para poder tratar su "adicción" (periodo durante el cual tuvo prohibido acercarse a una computadora).

Hoy en día Kevin Mitnick es uno de los hackers más reconocidos en el mundo entero, ha escrito varios libros, imparte conferencias en distintos países y cuenta con su propia empresa de seguridad llamada Mitnick Security (www.mitnicksecurity.com), la cual pone énfasis en la concientización como base para protegerse de ataques informáticos.

Como se ha podido comprobar, la ingeniería social es casi siempre una técnica de apoyo a otras técnicas, y mediante la suma de todas como ciertos atacantes logran sus objetivos. En ocasiones buscan una vulnerabilidad en el software, red o servidor, lo cual puede ser una tarea tediosa, que le lleve horas y horas, sin que haya garantía de tener éxito en la intrusión. Sin embargo, la vulnerabilidad puede estar en el factor humano, es decir, si la persona es vulnerable a estos ataques, será el eslabón más débil de la cadena que comprometa la seguridad de todo el sistema.

Las redes sociales, sobre todo si cuentan con un perfil público, pueden ser una mina de información para quien busca la pieza que le falta para poner en marcha su estrategia de ataque. Al ser una técnica de crackeo, la ingeniería social se logra a través de la manipulación psicológica y de las habilidades sociales, con el fin de obtener algún tipo de información sensible o datos útiles sin que la víctima sea consciente de su utilización maliciosa.

> "La persona que efectúa este método, trata de engañar a la víctima, buscando entrar en confianza o haciéndose pasar por alguien más, para obtener lo que necesita. Teniendo en cuenta que somos muy vulnerables y nos movemos a través de una serie de impulsos irracionales, el que ejecute esta técnica usará comúnmente el teléfono, el internet, el disfraz u otros métodos para engañar, fingiendo ser alguien más. En muchos de los casos que he conocido, la persona suplanta a un trabajador de la empresa o a alguien de servicio técnico", dice Emanuel Abraham, hacker ético de Security Solution & Education.

> "La ingeniería social no es una técnica cuadriculada. Depende de la malicia del atacante, así como de la que tenga la víctima. Se pueden utilizar infinidad de argucias y mañas para lograr la información que se necesita: desde sobornos a amigos y familiares para que faciliten el acceso a ella, hasta preguntas sueltas en ambientes de esparcimiento, correos electrónicos aparentemente inofensivos que hacen preguntas sencillas y cuyas respuestas interesan a quien solicita la información", sostiene la ingeniera Jacqueline Tangarife, gerente de Security Solutions & Education, empresa que es la representante exclusiva para Colombia de EC-Council Academia.

Conclusiones y Recomendaciones

Se debe tener en cuenta que a veces la persona que ataca no es tan buena o ni es un gran *hacker*, sino que las personas son muy vulnerables a ciertos ataques pues existe la costumbre de dejar a la vista de todos la información privada o la vida personal, es decir lo que hacemos a diario, a dónde vamos o con quién socializamos.

Hay un pensamiento muy real que dice "Que no existe nada más peligroso que una persona con información incompleta sacando sus propias conclusiones".

La mejor herramienta para protegerse de los ataques de ingeniería social es el **sentido común**. Con un pequeño esfuerzo de análisis de los ejemplos anteriores, podemos toparnos con las siguientes preguntas: ¿Es posible que un servicio usado por millones de personas como el MSN o el WhatsApp, tenga una vulnerabilidad que permita acceder al historial de conversaciones? ¿En verdad una entidad bancaria necesita confirmar nuestros datos para recibir dinero en una cuenta? ¿Es creíble que una compañía telefónica pueda perder los datos de sus clientes? ¿Es posible ser el ganador de un premio de lotería sin haber jugado?

Los siguientes consejos pueden ayudarle a identificar las estrategias usadas en la ingeniería social y por tanto, a evitar ser víctima de este tipo de ataques:

Nunca revele por teléfono o e-mail datos confidenciales (como claves de acceso, números de tarjetas de crédito, cuentas bancarias, entre otros).

Nunca haga click en un enlace a una página web que le llegue a través de un e-mail en el que le piden datos personales.

Desconfíe de cualquier mensaje de e-mail en el que se le ofrece la posibilidad de ganar dinero con facilidad.

Si es usuario de banca electrónica o de cualquier otro servicio que implique introducir en la web datos de acceso, asegúrese de que la dirección sea la correcta.

No confíe en las direcciones de los remitentes de e-mail o en los identificadores del número llamante en el teléfono, ya que pueden falsearse con suma facilidad.

Instale en su equipo un buen software de seguridad que incluya si es posible funcionalidad antivirus, antiphising, antispyware y antimalware para minimizar los riesgos.

Utilice el sentido común y pregúntese siempre que reciba un mensaje o llamada sospechosa, si alguien puede obtener algún beneficio de forma ilícita con la información que le solicitan.

Por último, una breve reflexión: la ingeniería social existe desde que el hombre es hombre, pues a fin de cuentas, simplemente se trata de conseguir que otra persona haga o diga lo que nosotros deseamos. Además, mucho antes del nacimiento de la red Internet, ya se utilizaban esas técnicas con propósitos deshonestos y con excelentes resultados, aunque nadie los había definido con el término de “Ingeniería Social”.

Bibliografía

Hadnagy, Christopher. (2011). Ingeniería Social. El Arte del Hacking Personal. (Anaya Mulmedia) (España)

Hector Jara y Federico G. Pacheco Ethical hacking, las técnicas de los hacker al servicio de la seguridad, Manuales Users.

Diario La Segunda, 26 de septiembre de 2011.

Kevin D. Mitnick y William L. Simon (2002). Human Element of Security. John Wiley & Sons. (Estados Unidos)

SirRoss. 19 de enero de 2005. A Guide to Social Engineering. (Estados Unidos)